Dc3 Digital Forensics Challenge

203 – Registry Analysis

Team Information

Team Name: elso-ren

Results Email: [redacted]

Examination Time Frame: to

Instructions

Description: Examiners must develop and document a methodology used to determine from the provided registry files and USB Image files located in the **203_Registry_Analysis_Challenge2008** folder, which of the USB devices was attached to the suspect hard disk drive. Report the exact registry key path, any additional entry information, the detailed explanation of your process (software or technique) used to examine and detect the information, and the reason for your selections.

Points will be awarded for successfully identified USB device connected to the suspect hard disk drive, provided you supply a detailed methodology of how you determined your findings.

Total Weighted Points: 40 Total Points available per entry – Total 200 Points Available

1. **Answers** – Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

Internal Reviewer Use Only

Reviewer:

Points Awarded:

Date:

Review Period: to

Completed: □ Yes □ No □ Partial

Question 203: Registry Analysis

Using Access Data's Registry Viewer 1.5.1.19, the registy files were examined. Based on the keys under SYSTEM\ControlSet001\Enum\USBSTOR\, all three USB tokens were connected. The key names contain the serial numbers provided. Full key paths are included below:

SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_Memorex&Prod_TD_Classic_003B&Rev_PMAP\0778102104F1&0

SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_Memorex&Prod_TD_Classic_003B&Rev_PMAP\0778102B05EC&0

SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_Memorex&Prod_TD_Classic_003B&Rev_PMAP\0778102C0211&0

@lso-ra@n